generating, by the black box server, the black box, such generated black box being unique and having a public / private key pair;

delivering, by the black box server, the generated black box to the DRM system; and

installing, by the DRM system, the delivered black box in such DRM system.

107. The method of claim 106 wherein the DRM system has a previously installed black box prior to the requesting step, the method further comprising determining prior to the requesting step that the previously installed black box is non-unique.

108. The method of claim 106 wherein the DRM system has a previously installed black box prior to the requesting step, the method further comprising determining prior to the requesting step that the previously installed black box is not current.

109. The method of claim 106 wherein the requesting step comprises requesting the black box by way of a network connection to the black box server.

110. The method of claim 109 wherein the requesting step comprises requesting the black box by way of an Internet connection to the black box server.

111. The method of claim 106 wherein the DRM system has a first previously installed black box prior to the requesting step, the first previously installed black box having a public / private key pair different from the public / private key pair of the generated black box, and wherein the generating step includes providing the generated black box with the public / private key pair of the first previously installed black box.

112. The method of claim 111 wherein the DRM system had a second previously installed black box prior to having the first previously installed black box, the second previously installed black box having a public / private key pair different from the public / private key pair of the first previously installed black box and also different from the public / private key pair of the generated black box, and wherein the generating step further includes providing the generated black box with the public / private key pair of the second previously installed black box.

113. The method of claim 106 wherein the generating step includes providing the generated black box with an identifier indicative of currency.

114. The method of claim 113 wherein the generating step includes providing the generated black box with a version number.

115. The method of claim 106 wherein the generating step includes providing the generated black box with a digital certificate.

11 10
116. The method of claim 115 wherein the generating step includes providing the generated black box with a digital certificate proffering that the generated black box should be trusted.

12 1
117. The method of claim 106 wherein the generating step includes encrypting at least a portion of the private key of the generated black box according to a code-based encryption technique.

13
118. The method of claim 117 wherein the generating step includes encrypting at least a portion of the private key of the generated black box according to software code associated with the generated black box, whereby adulteration of such software code prevents such private key from being decrypted.

14 1
119. The method of claim 106 wherein the generating step includes associating the generated black box with the DRM system / computing device, whereby the generated black box is inoperable on another DRM system / computing device.

15
120. The method of claim 119 wherein the requesting step includes providing information unique to the DRM system / computing device, and wherein the generating step includes generating the black box based in part on the provided information, whereby the

generated black box can recognize whether it is intended for the DRM system / computing device upon which it is installed.

121. The method of claim 119 wherein the DRM system / computing device is a first DRM system / computing device, wherein the generating step includes associating the generated black box with the first DRM system / computing device and also with a second DRM system / computing device, whereby the generated black box is inoperable on another DRM system / computing device which is not the first or second DRM system / computing device.

122. In combination with a digital rights management (DRM) system operating on a computing device, the DRM system requiring a black box for performing decryption and encryption functions, a method of obtaining the black box by the DRM system, the method comprising:

requesting the black box from a black box server, the black box server thereafter generating the black box, such generated black box being unique and having a public / private key pair;

receiving the generated black box from the black box server; and

installing the received black box in such DRM system.

123. The method of claim 122 wherein the DRM system has a previously installed black box prior to the requesting step, the method further comprising determining prior to the requesting step that the previously installed black box is non-unique.

124. The method of claim 122 wherein the DRM system has a previously installed black box prior to the requesting step, the method further comprising determining prior to the requesting step that the previously installed black box is not current.

125. The method of claim 122 wherein the requesting step comprises requesting the black box by way of a network connection to the black box server.

126. The method of claim 125 wherein the requesting step comprises requesting the black box by way of an Internet connection to the black box server.

127. The method of claim 122 wherein the DRM system has a first previously installed black box prior to the requesting step, the first previously installed black box having a public / private key pair different from the public / private key pair of the generated black box, and wherein the requesting step includes providing the public / private key pair of the first previously installed black box to the black box server, whereby the generated black box is provided with the public / private key pair of the first previously installed black box.

128. The method of claim 127 wherein the DRM system had a second previously installed black box prior to having the first previously installed black box, the second previously installed black box having a public / private key pair different from the public / private key pair of the first previously installed black box and also different from the public /

private key pair of the generated black box, and wherein the requesting step further includes providing the public / private key pair of the second previously installed black box to the black box server, whereby the generated black box is also provided with the public / private key pair of the second previously installed black box.

129. The method of claim 122 wherein the received black box includes an identifier indicative of currency.

130. The method of claim 129 wherein the received black box includes a version number.

131. The method of claim 122 wherein the received black box includes a digital certificate.

132. The method of claim 131 wherein the received black box includes a digital certificate proffering that such received black box should be trusted.

133. The method of claim 122 wherein at least a portion of the private key of the received black box is encrypted according to a code-based encryption technique.

134. The method of claim 133 at least a portion of the private key of the received black box is encrypted according to software code associated with such received black

box, whereby adulteration of such software code prevents such private key from being decrypted.

30 17
135. The method of claim 122 wherein the received black box is associated with the DRM system / computing device, whereby such received black box is inoperable on another DRM system / computing device.

31 31
136. The method of claim 135 wherein the requesting step includes providing information unique to the DRM system / computing device, and wherein the received black box was generated based in part on the provided information, whereby the received black box can recognize whether it is intended for the DRM system / computing device upon which it is installed.

32 31
137. The method of claim 135 wherein the DRM system / computing device is a first DRM system / computing device, wherein the received black box is associated with the first DRM system / computing device and also with a second DRM system / computing device, whereby the received black box is inoperable on another DRM system / computing device which is not the first or second DRM system / computing device.

33
138. In combination with a digital rights management (DRM) system operating on a computing device, the DRM system requiring a black box for performing decryption and

encryption functions, a method of providing the black box by a black box server, the method comprising:

receiving a request for the black box from the DRM system;

generating the black box, such generated black box being unique and having a public / private key pair; and

delivering the generated black box to the DRM system, the delivered black box being installed by the DRM system in such DRM system.

139. The method of claim 138 wherein the receiving step comprises receiving the request by way of a network connection between the black box server and the DRM system.

140. The method of claim 139 wherein the receiving step comprises receiving the request by way of an Internet connection between the black box server and the DRM system.

141. The method of claim 138 wherein the DRM system has a first previously installed black box prior to the requesting step, the first previously installed black box having a public / private key pair different from the public / private key pair of the generated black box, and wherein the generating step includes providing the generated black box with the public / private key pair of the first previously installed black box.

142. The method of claim 141 wherein the DRM system had a second previously installed black box prior to having the first previously installed black box, the second

previously installed black box having a public / private key pair different from the public / private key pair of the first previously installed black box and also different from the public / private key pair of the generated black box, and wherein the generating step further includes providing the generated black box with the public / private key pair of the second previously installed black box.

143. The method of claim 138 wherein the generating step includes providing the generated black box with an identifier indicative of currency.

144. The method of claim 143 wherein the generating step includes providing the generated black box with a version number.

145. The method of claim 138 wherein the generating step includes providing the generated black box with a digital certificate.

146. The method of claim 145 wherein the generating step includes providing the generated black box with a digital certificate proffering that the generated black box should be trusted.

147. The method of claim 138 wherein the generating step includes encrypting at least a portion of the private key of the generated black box according to a code-based encryption technique.

43 42
148. The method of claim 147 wherein the generating step includes encrypting at least a portion of the private key of the generated black box according to software code associated with the generated black box, whereby adulteration of such software code prevents such private key from being decrypted.

44 33
149. The method of claim 138 wherein the generating step includes associating the generated black box with the DRM system / computing device, whereby the generated black box is inoperable on another DRM system / computing device.

45 44
150. The method of claim 149 wherein the receiving step includes receiving information unique to the DRM system / computing device, and wherein the generating step includes generating the black box based in part on the received information, whereby the generated black box can recognize whether it is intended for the DRM system / computing device upon which it is installed.

46 44
151. The method of claim 149 wherein the DRM system / computing device is a first DRM system / computing device, wherein the generating step includes associating the generated black box with the first DRM system / computing device and also with a second DRM system / computing device, whereby the generated black box is inoperable on another DRM system / computing device which is not the first or second DRM system / computing device.

47
152. A computer-readable medium having computer-executable instructions thereon for performing a method in combination with a digital rights management (DRM) system operating on a computing device, the DRM system requiring a black box for performing decryption and encryption functions, the method for obtaining the black box by the DRM system and comprising:

requesting the black box from a black box server, the black box server thereafter generating the black box, such generated black box being unique and having a public / private key pair;

receiving the generated black box from the black box server; and

installing the received black box in such DRM system.

48 47
153. The method of claim 152 wherein the DRM system has a previously installed black box prior to the requesting step, the method further comprising determining prior to the requesting step that the previously installed black box is non-unique.

49 47
154. The method of claim 152 wherein the DRM system has a previously installed black box prior to the requesting step, the method further comprising determining prior to the requesting step that the previously installed black box is not current.

50 47
155. The method of claim 152 wherein the requesting step comprises requesting the black box by way of a network connection to the black box server.

156. The method of claim 155 wherein the requesting step comprises requesting the black box by way of an Internet connection to the black box server.

157. The method of claim 152 wherein the DRM system has a first previously installed black box prior to the requesting step, the first previously installed black box having a public / private key pair different from the public / private key pair of the generated black box, and wherein the requesting step includes providing the public / private key pair of the first previously installed black box to the black box server, whereby the generated black box is provided with the public / private key pair of the first previously installed black box.

158. The method of claim 157 wherein the DRM system had a second previously installed black box prior to having the first previously installed black box, the second previously installed black box having a public / private key pair different from the public / private key pair of the first previously installed black box and also different from the public / private key pair of the generated black box, and wherein the requesting step further includes providing the public / private key pair of the second previously installed black box to the black box server, whereby the generated black box is also provided with the public / private key pair of the second previously installed black box.

159. The method of claim 152 wherein the received black box includes an identifier indicative of currency.

160. The method of claim 159 wherein the received black box includes a version number.

161. The method of claim 152 wherein the received black box includes a digital certificate.

162. The method of claim 161 wherein the received black box includes a digital certificate proffering that such received black box should be trusted.

163. The method of claim 152 wherein at least a portion of the private key of the received black box is encrypted according to a code-based encryption technique.

164. The method of claim 163 at least a portion of the private key of the received black box is encrypted according to software code associated with such received black box, whereby adulteration of such software code prevents such private key from being decrypted.

165. The method of claim 152 wherein the received black box is associated with the DRM system / computing device, whereby such received black box is inoperable on another DRM system / computing device.

166. The method of claim 165 wherein the requesting step includes providing information unique to the DRM system / computing device, and wherein the received black box was generated based in part on the provided information, whereby the received black box can recognize whether it is intended for the DRM system / computing device upon which it is installed.

167. The method of claim 165 wherein the DRM system / computing device is a first DRM system / computing device, wherein the received black box is associated with the first DRM system / computing device and also with a second DRM system / computing device, whereby the received black box is inoperable on another DRM system / computing device which is not the first or second DRM system / computing device.

168. A computer-readable medium having computer-executable instructions thereon for performing a method in combination with a digital rights management (DRM) system operating on a computing device, the DRM system requiring a black box for performing decryption and encryption functions, the method for providing the black box by a black box server and comprising:

receiving a request for the black box from the DRM system;

generating the black box, such generated black box being unique and having a public / private key pair; and

delivering the generated black box to the DRM system, the delivered black box being installed by the DRM system in such DRM system.

169. The method of claim 168 wherein the receiving step comprises receiving the request by way of a network connection between the black box server and the DRM system.

170. The method of claim 169 wherein the receiving step comprises receiving the request by way of an Internet connection between the black box server and the DRM system.

171. The method of claim 168 wherein the DRM system has a first previously installed black box prior to the requesting step, the first previously installed black box having a public / private key pair different from the public / private key pair of the generated black box, and wherein the generating step includes providing the generated black box with the public / private key pair of the first previously installed black box.

172. The method of claim 171 wherein the DRM system had a second previously installed black box prior to having the first previously installed black box, the second previously installed black box having a public / private key pair different from the public / private key pair of the first previously installed black box and also different from the public / private key pair of the generated black box, and wherein the generating step further includes providing the generated black box with the public / private key pair of the second previously installed black box.

173. The method of claim 168 wherein the generating step includes providing the generated black box with an identifier indicative of currency.

174. The method of claim 173 wherein the generating step includes providing the generated black box with a version number.

175. The method of claim 168 wherein the generating step includes providing the generated black box with a digital certificate.

176. The method of claim 175 wherein the generating step includes providing the generated black box with a digital certificate proffering that the generated black box should be trusted.

177. The method of claim 168 wherein the generating step includes encrypting at least a portion of the private key of the generated black box according to a code-based encryption technique.

178. The method of claim 177 wherein the generating step includes encrypting at least a portion of the private key of the generated black box according to software code associated with the generated black box, whereby adulteration of such software code prevents such private key from being decrypted.

74

179. The method of claim 168 wherein the generating step includes associating the generated black box with the DRM system / computing device, whereby the generated black box is inoperable on another DRM system / computing device.

75 74

180. The method of claim 179 wherein the receiving step includes receiving information unique to the DRM system / computing device, and wherein the generating step includes generating the black box based in part on the received information, whereby the generated black box can recognize whether it is intended for the DRM system / computing device upon which it is installed.

76 74

181. The method of claim 179 wherein the DRM system / computing device is a first DRM system / computing device, wherein the generating step includes associating the generated black box with the first DRM system / computing device and also with a second DRM system / computing device, whereby the generated black box is inoperable on another DRM system / computing device which is not the first or second DRM system / computing device.

In the Abstract:

Please delete the Abstract and insert the following:

--A digital rights management (DRM) system operates on a computing device and requires a black box for performing decryption and encryption functions. To obtain the black box from a black box server, the DRM system requests such black box from such black box server. The black box server in response generates the black box, where such black box is